INTRODUÇÃO À ANÁLISE FORENSE EM REDES DE COMPUTADORES

CONCEITOS, TÉCNICAS E FERRAMENTAS
PARA "GRAMPOS DIGITAIS"

Ricardo Kléber M. Galvão

Novatec

Editor: Rubens Prates
Capa: Carolina Kuwabata/Ricardo Kleber Galvão
Revisão gramatical: Marta Almeida de Sá
Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-307-9

Histórico de impressões:

Novembro/2013 Primeira edição

Novatec Editora Ltda.
Rua Luís Antônio dos Santos 110
02460-000 – São Paulo, SP – Brasil
Tel.: +55 11 2959-6529
Fax: +55 11 2950-8869
Email: novatec@novatec.com.br
Site: www.novatec.com.br
Twitter: twitter.com/novateceditora
Facebook: facebook.com/novatec
LinkedIn: linkedin.com/in/novatec
MP20131106

CAPÍTULO 1

Computação forense

Este capítulo abrange os principais conceitos relacionados à computação forense, contextualizando o assunto principal deste livro ao analisar a diferença entre os procedimentos e as ferramentas relacionados à análise forense computacional "tradicional", focada na perícia em mídias, e a análise forense computacional em redes de computadores.

1.1 Principais conceitos relacionados à computação forense

A perícia forense é o suporte técnico ao judiciário, realizado preferencialmente por pessoas com formação e capacidade para isso nas mais diversas áreas do conhecimento, para a resposta a quesitos para os quais o judiciário não dispõe de embasamento suficiente para julgar com precisão.

Esse suporte técnico é dado pelo perito designado para, utilizando sua *expertise* na área específica, periciar o objeto da investigação e apresentar respostas a quesitos na forma de laudo ou parecer técnico.

Nesse contexto, a perícia forense em computação, ou computação forense, pode ser definida, de forma superficial, mas direta, como a área da computação responsável por dar respostas ao judiciário em questões envolvendo sistemas computacionais, sejam os objetos da investigação equipamentos, mídias, estruturas computacionais ou que tenham sido utilizados como meio em atividades sob investigação. Envolve, pois, a obtenção e análise de informações digitais e/ou equipamentos, infraestrutura e mídias computacionais para o uso como evidências em casos cíveis, criminais ou administrativos.

Existem, atualmente, muitos livros contendo definições mais completas e detalhadas sobre computação forense. Para subsidiar o assunto tema deste livro é suficiente, porém, a definição apresentada e a distinção, a seguir, de ambientes estáticos e voláteis como objeto de perícia na área.

É importante deixar claro que computação forense não se restringe à recuperação de dados, procedimento que envolve a recuperação de informações de computadores ou mídias que tiveram dados apagados e/ou escondidos proposital ou intencionalmente, em que o objetivo é apenas o de recuperar a maior quantidade possível de arquivos perdidos, sem a preocupação, por exemplo, com a preservação das mídias envolvidas para uma possível investigação dos motivos que levaram à perda de dados e até mesmo indícios sobre usuários ou processos envolvidos no incidente.

Situações nas quais seja necessário o suporte da computação forense para procedimentos de recuperação de dados vão muito além do uso de ferramentas de recuperação; envolvem toda uma estratégia de suporte com foco na preservação de evidências, definição prévia de técnicas e ferramentas, coleta e análise de dados, primando pela integridade e pelo detalhamento dos processos utilizados, finalizando com um laudo ou parecer técnico sobre todo o processo.

Casos em que seja necessário o uso da computação forense (em processos cíveis ou criminais, por exemplo) podem resultar na condenação ou absolvição de pessoas investigadas em processos em que houve direta ou indiretamente o uso de recursos computacionais na consecução dos atos investigados e para os quais o judiciário não dispunha de conhecimento técnico suficiente para julgar com precisão.

1.1.1 Terminologia

Embora não seja objetivo deste livro detalhar conceitos e técnicas de computação forense em geral – isso desviaria o foco da análise forense em redes de computadores, indo além do conhecimento necessário para subsidiar este tema –, alguns conceitos relacionados à terminologia adotada na prática da computação forense merecem a citação e definição como complemento.

- **Mídia de provas**: engloba todas as mídias que são objeto de investigação, incluindo os dispositivos convencionais e não convencionais de armazenamento de dados (discos rígidos, pendrives, cartões de memória ou qualquer dispositivo capaz de armazenar dados) e dispositivos/meios responsáveis pelo armazenamento e/ou a transmissão de dados voláteis (memórias voláteis e infraestrutura de redes cabeadas ou sem fio).

- **Mídia de destino**: imagem pericial fidedigna das mídias de provas armazenadas com proteção contra alterações (qualquer procedimento de leitura e/ou gravação que implique em modificação de seus dados) de modo a permitir a verificação de sua integridade e quantas cópias forem necessárias para análise pericial sem a necessidade de novamente se recorrer às mídias de provas.

- **Análise ao vivo**: atividade pericial realizada diretamente sobre as mídias de provas. Esse tipo de perícia geralmente é realizado quando não se dispõe de recursos e/ou tempo e/ou autorização para a adequada geração da mídia de destino e análise posterior. Embora, nesses casos, os resultados (respostas aos quesitos) sejam mais rápidos, esses resultados são passíveis de contestação judicial em função da impossibilidade de nova perícia posterior por falta de mídia de destino e, naturalmente, alteração das mídias de provas. A análise ao vivo realizada sem alterar as mídias de provas (garantindo a impossibilidade de modificação de mídias de armazenamento durante a perícia, por exemplo, e impedindo a manipulação posterior dessas mídias até que nova perícia possa ser realizada) é uma exceção à citada possibilidade de contestação.

- **Análise post-mortem (offline)**: metodologia de perícia mais recomendada e mais utilizada em computação forense, em que a análise é feita sobre as mídias de provas ou até sobre uma cópia dessas mídias, permitindo maior flexibilidade nos procedimentos de análise dos dados sem comprometer a mídia original (mídia de provas).

1.1.2 Perícias públicas e privadas

Em um primeiro momento, pode-se classificar análises forenses computacionais em duas categorias distintas:

- **Análise forense computacional em investigações públicas**: ligadas à investigação em processos criminais, com a participação de perito oficial ou cível, formalmente constituídas e levadas à justiça.
- **Análise forense computacional em investigações privadas ou corporativas**: ligadas à investigação em processos de interesse particular de pessoas ou empresas, não necessariamente envolvendo o judiciário, com a participação de perito ad-hoc.

1.1.3 Sistematização de procedimentos periciais

Vários podem ser os fatores que determinam o que deve ser considerado na preparação para a análise e consecução de um processo que envolve a necessidade do uso da computação forense. Na falta de normatização específica sobre os passos a serem seguidos na preparação para a análise pericial, sugere-se, a seguir, uma lista de detalhes que devem ser observados.

- **Amparo legal** (perito não é advogado nem juiz): existe habilitação legal para o acesso e a manipulação de todos os equipamentos, softwares, redes e ambientes (físicos) envolvidos? Em muitos casos, existe a necessidade de mandados, licenças para utilização de softwares e/ou assinatura de termos de anuência de modo que nenhum dos passos da atividade pericial infrinja normas ou direitos de pessoas e instituições.
- **Periculosidade** (perito não policial): existe segurança suficiente para a manipulação dos dados envolvidos sem a iminente possibilidade de coação ou ameaças à atividade pericial ou mesmo à integridade física do perito? Mesmo com suporte de contingente policial, deve-se, sempre que possível, evitar a exposição do perito. Em casos mais críticos, indica-se a realização de treinamento de agentes para a manipulação e coleta de dados em locais de alta periculosidade, cabendo ao perito apenas os procedimentos de análise de evidências em local seguro e adequado.

- **Conhecimento técnico**: a formação em área específica, mesmo com pós-graduação, nem sempre é garantia de *expertise* suficiente para tratar com todas as necessidades envolvidas em um caso para o qual se solicita o suporte pericial. É importante e fundamental que o perito tenha o discernimento de não aceitar a realização de uma perícia ou solicitar auxílio de colegas com maior preparo para os desafios da atividade pericial em cada caso quando não se sentir apto para executar adequadamente todos os passos necessários para a sua realização. Essas situações tornam-se mais graves quando se trata de perito oficial, que, provido de fé pública, por excesso de preciosismo, vaidade ou comodidade, pode incorrer em falsa perícia por falta de conhecimento com consequências provavelmente e geralmente desastrosas.

- **Planejamento**: iniciar um processo de perícia sem o suporte material adequado é, no mínimo, inconsequente. Mídias para armazenamento, equipamentos com processamento e memória suficientes, cabos, conectores, ativos de rede, embalagens para acomodação segura de mídias, veículos apropriados para transporte, local para acomodação provisória de equipamentos que serão periciados posteriormente e softwares adequados precisam ser dimensionados e providenciados antes do início das atividades. Além disso, o número de pessoas envolvidas nos procedimentos de coleta e análise precisa ser definido e providenciado, sempre que possível, com antecedência. É comum, ainda, que o planejamento inicial necessite de ajustes após o início das atividades periciais em função de necessidades surgidas durante os procedimentos de coleta de evidências.

- **Cadeia de custódia**: o registro detalhado de todos os passos, pessoas, ambientes, mídias e informações direta ou indiretamente relacionadas à perícia é fundamental para instrumentar o processo e dar suporte a investigações ou contestações posteriores sem que todo o processo pericial necessite ser novamente realizado.

- **Laudo/parecer técnico**: o perito deve escrever o resultado da análise pericial de modo que os interessados e responsáveis pelo julgamento do mérito entendam perfeitamente sem a necessidade de conhecimento técnico (já que isso motivou a requisição da perícia

especializada) e sem o risco de interpretação equivocada em função dos termos utilizados ou pouco detalhamento nas respostas aos quesitos. O laudo pode (e em muitos casos, deve) ser enriquecido com desenhos, imagens e analogias para que mesmo pessoas leigas no assunto entendam com clareza o resultado da perícia realizada.

1.2 Análise forense computacional em mídias

A grande maioria das atividades periciais em computadores tem como objetivo a análise de mídias de armazenamento (discos rígidos internos e externos, pendrives, CDs, DVDs, cartões de memória flash de vários tipos e a própria memória com suas informações voláteis armazenadas temporariamente) em processos de recuperação e extração de arquivos, classificação e busca de evidências após a coleta e identificação realizados de forma adequada. Esse tipo de atividade é a análise forense computacional "tradicional", que, embora tenha muitos detalhes importantes que devem ser considerados e apresentados quando o assunto é computação forense, não será detalhada neste livro em função de tratar-se de outra modalidade, diferente (pelo menos conceitualmente) do assunto principal aqui abordado.

Os procedimentos padrões, em perícias em ambientes computacionais, têm sequências sugeridas semelhantes, porém, existem algumas particularidades em cada tipo (perícia tradicional ou em redes) que merecem cuidado na apresentação dos conceitos envolvidos. Em função disso, os conceitos apresentados neste livro, embora se assemelhem em alguns casos com os conceitos relacionados à perícia tradicional, terão sempre o foco na análise forense em redes de computadores, com detalhes, ferramentas e procedimentos apresentados sempre nessa abordagem.

1.3 Análise forense em redes de computadores (network forensics)

Análise forense em redes de computadores consiste na captura, no armazenamento, na manipulação e na análise de dados que trafegam (ou trafegaram) em redes de computadores, como parte de um processo investigativo.

É importante que esteja claro que análise forense em redes de computadores:

- **Não é um produto**, é um processo que envolve conhecimento técnico, uso de ferramentas apropriadas, raciocínio e amparo legal;
- **Não substitui soluções de segurança** (como firewalls, IDS e antivírus) nem processos (políticas de segurança e uso de recursos computacionais);
- **Não envolve somente a captura de tráfego**, mas, de forma complementar, análise de registros de logs de acesso a sistemas, firewalls, IDS, servidores de aplicações etc.

1.3.1 Questões iniciais

Antes mesmo do início de qualquer procedimento técnico, do uso de ferramentas ou da manipulação de evidências, é necessário refletir e definir estratégias de abordagem em função das respostas a questões importantes nessa fase como:

a. Que equipamentos serão analisados, quais os seus sistemas operacionais e que tipo de tráfego passa por cada um deles?

b. Qual quantidade pode/precisa ser capturada para análise?

c. É possível utilizar filtros já no processo de captura sem comprometer a análise posterior por falta de dados descartados com a filtragem?

d. Como garantir a privacidade de dados que não fazem parte do processo (sobre os quais não se tem amparo legal para manipulação, por exemplo)?

e. Como garantir a integridade dos dados após a captura?

f. Será necessário realizar análise de dados durante o processo de captura (tempo real) ou é possível armazenar os dados capturados para análise posterior?

g. Os quesitos estão bem formulados? Tendo em vista o resultado esperado da perícia, e considerando que o solicitante em alguns casos não dispõe de conhecimento técnico suficiente para elaborar os quesitos adequados, não existe a necessidade da sugestão de novos quesitos ao solicitante antes do início da atividade pericial?

Mesmo que os procedimentos sugeridos (questões iniciais) possam implicar em atraso no início dos procedimentos técnicos relacionados à perícia, a não observância desses detalhes pode atrasar muito mais (ou até inviabilizar) o prosseguimento das atividades periciais por falta de equipamentos, mídias ou conhecimentos adequados durante os procedimentos periciais.

1.3.2 Questões a considerar durante a realização de perícias em redes

Com a devida cautela, após analisados os pontos importantes levantados durante o planejamento da atividade pericial, existem outras questões que devem ser consideradas durante todo o processo de perícia:

a. **Em casos em que a análise será feita após a coleta, o método de coleta é o adequado para a reconstrução de sessões e arquivos?** Para isso é necessário que pelo menos parte do material coletado seja analisado durante o processo de coleta simulando os procedimentos que serão feitos posteriormente para, se for o caso, adequar os parâmetros utilizados na(s) ferramenta(s) utilizada(s) para a captura de dados.

b. **A coleta de evidências está sendo feita de modo a garantir a reconstrução cronológica de sessões?** Isto é fundamental em casos, por exemplo, de incidentes de segurança em que estão sendo investigados o nível de comprometimento de equipamento(s) e os prováveis passos do responsável por esse comprometimento.

c. **A associação entre os dados coletados e endereços IP de origem e destino, além de informações sobre data e hora em que os dados trafegaram na rede, está sendo realizada?** Eventuais arquivos e informações encontrados, por mais "interessantes" que possam parecer os seus conteúdos, não têm

valor algum por si só. Devem estar acompanhados da identificação dos responsáveis pelo envio e recebimento, além das informações complementares como protocolos/serviços utilizados e dados temporais.

d. **A privacidade está sendo respeitada, também, nos processos de captura e análise?** É preciso utilizar ferramentas que permitam a filtragem de dados sem a intervenção/análise humana de modo que informações sobre pessoas e processos sobre os quais não se tem autorização legal para visualização, análise ou manipulação sejam removidas ou omitidas dos dados que serão analisados manualmente. A constatação/prova de visualização de dados privados (sob os quais não se tinha autorização legal para manipulação) pode comprometer tanto a investigação quanto o próprio perito envolvido.

e. **Os dados capturados estão sendo convenientemente armazenados, identificados e "assinados"**? A volatilidade dos dados que trafegam em redes faz destes procedimentos uma das partes mais importantes do processo. Gravar adequadamente e assinar digitalmente os dados capturados fará toda a diferença nas próximas fases da atividade pericial.

f. **Existem testemunhas para atestar a captura?** O perito oficial tem fé pública, ou seja, respaldo legal para capturar e assinar o arquivo de captura sem a probabilidade de contestação posterior quanto à veracidade dos dados (acusação de manipulação posterior com supressão ou inclusão de informações). A perícia ad-hoc, feita por perito não oficial, necessita da assinatura de testemunhas para a validade do arquivo de captura como parte do processo, sob pena de contestação de todo o processo de captura.

Realizado o planejamento, definida a abordagem, providenciados os equipamentos adequados e mídias para armazenamento e escolhidas as ferramentas, é importante, ainda, definir o que deve ser capturado/analisado, e, para isso, deve-se conhecer plenamente o que pode ser analisado em um processo de perícia em redes de computadores.

1.3.3 Objetos da análise nas perícias em redes de computadores

A definição dos objetos que precisam ser analisados implica diretamente na escolha das técnicas, das ferramentas, dos equipamentos e da infraestrutura para a execução de perícias em redes de computadores. A seguir são apresentados os objetos de análise que podem ser, isoladamente ou em conjunto, o alvo da investigação.

a. **Conteúdo total dos dados (full content data)**: implica na coleta de todos os bits de informação contidos nos pacotes em tráfego, tanto os cabeçalhos como as cargas (payload) em todas as camadas da pilha TCP/IP. Assim, nesse tipo de perícia, o objeto da análise são os endereços de rede, as portas, os dados de sinalização e controle, além de informações de logins/senhas (quando for o caso), arquivos de imagens, documentos, comandos digitados, requisições e respostas a serviços.

b. **Conteúdo parcial dos dados (partial content data)**: a partir da definição de parâmetros de filtragem (BPFs por exemplo), o objeto neste caso são todos os dados de sessões relacionadas às informações do filtro. Todos os pacotes que "casarem" com o padrão apresentado no filtro devem ser capturados/analisados integralmente (cabeçalho e payload). Esse filtro tanto pode conter dados de origem/destino e/ou portas/serviços acessados como pode fazer referência a períodos de tempo, como o tráfego total em uma data e hora específica, ou ainda a nomes de usuários ou palavras-chave.

c. **Registros em logs**: nesses casos, a perícia não é realizada diretamente sobre os pacotes em tráfego, mas sobre os registros (logs) relacionados a alguma aplicação que utiliza ou utilizou a rede, como logs de: firewalls, sistemas de detecção de intrusões (IDS), servidores de aplicação (logs registrados por servidores web [HTTP], proxies, FTP, e-mails [SMTP, POP3/IMAP], dentre outros serviços), sistemas operacionais, tabelas/registros ARP e registros feitos pelos próprios sistemas operacionais relacionados a uso de recursos de rede.

1.3.4 Desafios da análise forense em redes de computadores

Os desafios da perícia estão diretamente ligados aos detalhes identificados no planejamento, na coleta e na análise em redes. Em linhas gerais, deve-se buscar, o quanto antes, determinar:

- **Origem dos dados**: identificação da abrangência do ambiente sob investigação e do conteúdo das redes que por ele trafegam dados;
- **Granularidade dos dados**: nível de detalhes que precisam ser coletados/analisados (pacotes completos ou somente os cabeçalhos)?;
- **Integridade dos dados**: o resultado da perícia ficará comprometido caso haja descarte de parte dos pacotes (por limitações de hardware/software, por exemplo)?;
- **Condição de evidência legal dos dados**: o resultado da perícia será aceito pelo judiciário (quando for o caso)?;
- **Privacidade dos dados**: a coleta/análise pode ser realizada com a garantia de que o perito tem autorização para manipular todos os dados que lhe forem apresentados, ou seja, as informações sensíveis, para as quais não se tem autorização para manipular, têm sua privacidade garantida?;
- **Análise dos dados**: em função do volume e da complexidade de análise dos dados é necessário buscar garantir a automatização de parte dos processo utilizando ferramentas específicas sem comprometer o resultado da perícia, buscando soluções que realizem a manipulação de dados brutos de forma rápida e automatizada, interagindo com o perito, sempre que possível, por meio de interfaces "amigáveis" de alto nível.

Para dar suporte conceitual e técnico às informações importantes que podem/devem ser analisadas em atividades de análise forense em redes de computadores o capítulo 2 apresenta conceitos, funcionamento e detalhes sobre os principais protocolos passíveis de captura e análise em redes de computadores, com foco na pilha de protocolos TCP/IP, padrão na internet e nas redes locais a ela interconectadas.